AFFIDAVIT

I, Ashley Davis, Special Agent with the Federal Bureau of Investigation (FBI), Kansas City, Missouri, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent for the FBI since January 2007. As part of my duties as a Special Agent, I am assigned to investigate violations of federal law, specifically the online exploitation of children. This includes violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have had numerous hours of professional law enforcement training in the detection and investigation of criminal offenses. I have written, executed, and/or participated in the execution of numerous search warrants. Specifically pertaining to the area of child pornography and child exploitation investigations, I have gained expertise in these investigations through training, discussions with other law enforcement officers, and everyday work related to conducting these types of investigations.

2. I am investigating violations of 18 U.S.C. § 875(d), that is, extortion, and 18 U.S.C. § 371, that is, conspiracy to commit extortion, occurring in the Western District of Missouri and elsewhere. This affidavit is made in support of an application for a warrant to search the places described in Attachment A, that is the premises located at 8511 Kentucky Avenue, Raytown, Missouri 64138 (hereafter the "SUBJECT PREMISES"), as well as the person of ISAIAH LEWIS, for the items described in Attachment B. As will be shown below, there is probable cause to believe LEWIS, residing at the SUBJECT PREMISES, has committed the offense of extortion, in violation of 18 U.S.C. § 875(d), as well as conspiracy to commit extortion, in violation of 18 U.S.C. § 371. I am submitting this affidavit in support of a search warrant of the SUBJECT PREMISES, and the person of LEWIS, for items constituting

instrumentalities, fruits, and evidence of the foregoing violations. I am requesting authority to search the entire premises, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits and evidence of crime.

3. This affidavit is based upon information I have gained from my investigation, my training and experience, as well as information obtained from conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of 18 U.S.C. § 875(d) are presently located at the SUBJECT PREMISES at 8511 Kentucky Avenue, Raytown, Missouri 64138.

STATUTORY AUTHORITY

4. This investigation concerns alleged violations of 18 U.S.C. § 875 (d) and 18 U.S.C. § 371, relating to extortion and conspiracy to commit extortion.

a. 18 U.S.C. § 875 (d) prohibits a person from transmitting in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, with the intent to extort from any person, firm, association, or corporation, any money or other thing of value.

b. 18 U.S.C. § 371 prohibits two or more persons conspiring to commit any offense against the United States, in such a case where one or more of such persons do any act to effect the object of the conspiracy.

BACKGROUND OF THE INVESTIGATION

5. On October 12, 2022, Affiant received information from Special Agent Karen Ryndak, FBI Headquarters, Child Exploitation Operations Unit (CEOU), concerning ISAIAH LEWIS. SA Ryndak advised that CEOU was notified by a representative of Meta Platforms, Inc.[1] about concerning communications between LEWIS and an individual utilizing the name "Jenny Glenn" on Facebook Messenger. In these communications, LEWIS made several references to being involved in a fraud scheme, and also discussed the suicide of a 14-year-old male. The internet protocol (IP) addresses associated with user "Jenny Glenn" provided by Meta Platforms, Inc., resolved back to Lagos, Nigeria[2]. Meta Platforms, Inc. also provided IP address 2601:300:4000:9f20:28aa:387b:d45a:1929 for LEWIS, which was captured on September 29, 2022 at 1:14AM PDT.

6. Affiant reviewed the following excerpts from the communications between LEWIS and "Jenny Glenn," which took place between July 22, 2022 and September 20, 2022. Within the communication between LEWIS and "Jenny Glenn," it appears that the two are discussing the transferring of currency from other persons to LEWIS, and then to "Jenny Glenn" using various currency transfer applications such as Venmo or CashApp. LEWIS and "Jenny Glenn" also discuss the suicide of a 14-year-old male after he was forced to send money to another individual, and LEWIS's potential involvement with that situation. LEWIS also refers to a law enforcement investigation into their activities, and a desire to potentially kill a person known as "Lena" for her involvement.

[1] Meta Platforms, Inc. is an American multinational technology conglomerate based on Menlo Park, California. It was formerly known simply as Facebook, but now collectively owns Facebook, Instagram, and WhatsApp, among other products.

[2] CEOU currently has an active investigation involving the sexual exploitation of minor victims over social media applications. There are numerous unknown subjects utilizing various usernames/accounts to communicate with these minor victims. Based on the investigation to date, these subjects are believed to reside in Nigeria.

July 22, 2022

Jenny Glenn: Hello sir
Can you send me your cashapp,PayPal and zelle tag
My friends wants to be sending me money once in a while for feeding

LEWIS: Sending money to me

Jenny Glenn: You will send it back to me through btc[3]
Just like $20 or $50 once in a while tho
I want to be saving up for both me and diane since I am renting a new house

LEWIS: Ok
My number 8167087146

Jenny Glenn: Uhm ok
Your tags?

LEWIS: isaiahkidlovechicken@gmail.com
I'm using zelle

Jenny Glenn: This your zelle right?

LEWIS: Yes

Jenny Glenn: Your cashapp also

LEWIS: Why

Jenny Glenn: I could use anyone
So I will just send you a screenshot
And PayPal

LEWIS: I'm using only zelle because it's the only thing I know Won't need btc
It's easy for you to try to use btc and it never send

Jenny Glenn: Wait I might be sending $50 to your cashapp

[3] "BTC" commonly refers to bitcoin, a cryptocurrency.

LEWIS: Tell them send 50 to zelle I don't want the to question sending me btc

Jenny Glenn: No chill did you not read what I was saying
My friend could use zelle or cashapp orpaypal she wants and since she's just helping me send little token I am saving up for me and diane
I can't argue with her
Sometimes she might say her zelle down I should give her PayPal
So it's anyone she wants I will give her

LEWIS sent a screenshot of a payment confirmation. The message read "H.N.I.C. Reed. Payment from $HNICReed $100 Today at 6:26 PM.

Jenny Glenn: 1S8TYV9WWcPp8EnD5s4kGwfbQGyaxeegB
Please send to my wallet sir

July 26, 2022

Jenny Glenn: Let me see screenshot please
She sent $350
Then $500 then $200
Then she also sent $70

LEWIS sent a screenshot of credit activity to a Zelle account ending in 4805, associated with U.S. Bank. A message on the screenshot read, "A deposit of $200 from Antonio Davis was deposited in your account." The received date was July 26, 2022.

Jenny Glenn: Ok you saw the $500, $350 and $200
With the $70 too
So that's $1120

LEWIS sent a screenshot of a message indicating a payment of $200 sent by Antonio Davis on July 26, 2022 had failed.

Jenny Glenn: It shows $1120

LEWIS: Wait

Jenny Glenn sent a screenshot of several recent transactions from an Advantage Banking account ending in 0785. Two of these transactions were Zelle transfers from "Isaiah" in the amount of $350 and $500.

LEWIS: I'm unable to screen shot bank accounts

Jenny Glenn: Just history?
I just want transparency
Would you rather give me your email and password incase next time you are asleep and she sends money
$MattyBoo487
Request $40 from her cashapp please

LEWIS sent a screenshot of a pending payment request for $40, sent to Matthew Stephens, account $MattyBoo487.

Jenny Glenn: Help me request another $40 please
$X3Skeppy
Request $800
I really wanted to make up for my 1120
She said I should give her venmo
If she sends $800 through venmo you will take $20

LEWIS: Got venmo up

Jenny Glenn: Okay send it
Your venmo fast

LEWIS sent a screenshot of a Venmo account, identified as display name Isaiah Lewis, unique username @Isaiah-Lewis-111.

August 02, 2022

LEWIS: No more cashapp

Jenny Glenn: Wait she used cashapp??

LEWIS: Zelle paypal only
I told you cashapp only works with people I know not a single person gave me their number

Jenny Glenn: Sec1899@yahoo.com
Add him to your cashapp immediately

LEWIS sent a screenshot of an account in the name of Samuel Curtis, username $curtdog777. This user was not in LEWIS'S contacts. A failed payment of $120 is visible at the bottom of the image.

Jenny Glenn: Can't you add the mail to your contacts?
+1 (401) 290-8148

August 04, 2022

LEWIS sent a screenshot of a Zelle deposit associated with U.S. Bank. A partial message on the screenshot read, "A new payment of $290 from Stephanie Galindo was deposited in…."

Jenny Glenn: Okay send
Take $20

LEWIS: You're using my bank acc

Jenny Glenn: Before she sends the $5000 she said you should screenshot your zelle mail all at once the whole of it not like this
Screenshot your zelle history please I want to calculate all the money that entered from yesterday

August 09, 2022

LEWIS: Bank called 5 fraud claims
Lena doing something and not telling me
This is real people being frauded
These multiple accounts money being sent by
Someone of them are innocent people
This is bad extremely bad
This Is a scam
And she involved me in this
And I'm taking all the blame

Jenny Glenn: Who's tracking you
Stop scaring me please

LEWIS: Us bank
Like I said because of you I can't use zelle and I am being watched by us bank

Jenny Glenn: Just use cashapp next week
It should have been cleared by then

August 23, 2022

LEWIS: I still going a sheriff came to my house about fraud claims
Saying I'm a victim of fraud
Are you from south Carolina

Jenny Glenn: Not from South Carolina
Maybe the person that was giving her money is from South Carolina
What tf did the sheriff say

LEWIS: A boy killed himself and say he a victim to the fraud but I'm no victim and if I was I immediately cut off

Jenny Glenn: Hope it's nothing related to jail?

LEWIS: If anything I'm relieved since they think I'm a innocent person
They're unauthorizing money I'm my account
Putting claims

Jenny Glenn: You in the bank rn?

LEWIS: Not yet but I can't imagine nothing good from the papers
And the county sheriff coming to my home

Jenny Glenn: Let me see the papers

LEWIS sent a picture of three hard copy letters from US Bank, indicating his account ending in 4805 was the beneficiary of three authorized transactions in the amount of $140, $200, and $150. These transactions occurred on July 31, 2022 and August 01, 2022.

LEWIS: I was supposed to protect him from this now they saying that someone force someone to give him money
That woman

LEWIS sent a screenshot of a text conversation between himself and Special Agent (SA) Millie Agrawal, South Carolina Law Enforcement Division. LEWIS asked SA Agrawal , "Can you tell me when they force them to send money to me." SA Agrawal replied, "We only looked

for transactions on the dates of our incident, which was 7/26 and 7/27, and we saw a $25 transfer from our victim, and an $800 transfer from another potential victim."

LEWIS: Here's more information
She stole money from 2 victims and put it in my zelle
We can try to get his zelle back but besides that not really except convince lena to give us the contacts us that women before killing her

Jenny Glenn: I will make sure to get the contact before we kill her
You sure bout getting his zelle back?

LEWIS: No

Jenny Glenn: Why

LEWIS: Because it's been connected to a suicide of a 14 year old
The women forced the kid to transfer money to his zeĺle
The stress of loosing 800 dollars was too much

August 24, 2022

LEWIS: I'm not afraid of killing someone I'm afraid of getting caught and looking cece
But they trace me from 2 out of 50 transfers
So I'm not so worried
I can easily hide so they can't trace me like temporary block
I didn't even have a reaction with the 14 year old kid dying
Nor care
Even though it's connected by me

August 27, 2022

LEWIS: So basically we found out her actions led a 14 year old boy to kill themselves and frame it on me so I want to gather info on her and who she worked with that framed me so the police can look into it I still want lena dead but I want to talk to her before but idk how without making seem stupidly obvious for what I'm trying to do

7. On October 13, 2022, Affiant made contact with Deputy Miller, Jackson County Missouri Sheriff's Office, regarding LEWIS. Deputy Miller indicated he had received a request from SA Agrawal, who was working an investigation involving a minor victim in South Carolina. SA Agrawal requested assistance from Deputy Miller in locating LEWIS to provide him with her contact information. Deputy Miller indicated he met with LEWIS at the SUBJECT PREMISES on August 23, 2022 (the same date Lewis sent the above message stating he had met with a Sheriff) and provided him with SA Agrawal's information. At the time Deputy Miller made contact with LEWIS, he was living at the SUBJECT PREMISES with his mother.

8. On October 13, 2022, Affiant telephonically contacted SA Agrawal regarding LEWIS. SA Agrawal indicated she had investigated the suicide of a 17-year-old male (hereafter "MV") located in South Carolina, which occurred around 1:40AM on July 27, 2022. Upon reviewing the Instagram application in the MV's phone, SA Agrawal made note of communications between MV and an individual with the username bellajannet28, which began around 9:00PM on July 26, 2022. Bellajannet28 purported to be a 19-year-old female and requested nude images of MV. MV sent bellajannet28 at least one image of his genitalia. After receiving this image, bellajannet28 began extorting MV for money, and threatened to send the image to MV's family members if he did not comply. Bellajannet28 also provided MV with the Venmo account Isaiah-Lewis-111 and MV immediately sent $25 to the account. Bellajannet28 continued to threaten MV if he did not send more money and told MV he had until Monday to send $75 more. Less than 20 minutes later, MV committed suicide. On August 10, 2022, a search warrant was obtained for customer information associated with the Isaiah-Lewis-111 Venmo account. Venmo subsequently identified the customer as ISAIAH LEWIS, DOB December 26, 2003, Social Security Account Number XXX-XX-6306, address 8511 Kentucky Avenue,

Raytown, Missouri 64138, email address isaiahkidlovechicken@gmail.com, telephone number (816) 708-7146. A financial account ending in 4805 from U.S. Bank was also associated with the Venmo account.

9. On October 13, 2022, Affiant telephonically contacted Comcast Cable Communications and requested an emergency disclosure pertaining to IP address 2601:300:4000:9f20:28aa:387b:d45a:1929 on September 29, 2022 at 1:14AM PDT. Comcast immediately identified the subscriber as Jannis Lewis, 8511 Kentucky Avenue, Raytown, Missouri 64138, the SUBJECT PREMISES.

10. Based on intelligence gathered about Nigerian criminal organizations, CEOU has identified commonalities in traditional sextortion schemes and financially motivated sextortion schemes. Traditionally, the goal of subjects committing sextortion was to utilize victims' images to obtain more child sexual abuse material (CSAM). In addition, traditional sextortion schemes mainly targeted minor females. In contrast, the goal of financially motivated sextortion was to obtain and utilize CSAM to extort money, in various forms, from victims. Additionally, financially motivated sextortion mainly targeted minor males, ages 14 to 17. CEOU observed the following trends unique to financially motivated sextortion:

A. A high rate of suicide in minor male victims of financially motivated sextortion schemes. In contrast to traditional sextortion, victims of financially motivated sextortion committed suicide within a relatively short time period, sometimes within hours, of the sextortion occurring. In addition, after the victim committed suicide, subjects began to extort family members for money utilizing the CSAM of victims.

B. Once subjects obtained CSAM, they demanded money in the various forms, such as gift cards, Paypal, Cashapp, Venmo, and Zelle.

C. A majority of the actors were located in Nigeria.

D. Subjects sometimes utilized United States citizens as "money mules" as a means to avoid detection. The subjects would generally identify and utilize individuals to serve as "money mules," and the subjects would then direct the victims to submit payment directly to the "money mule's" account. The "money mule" would then transfer the funds from their account to the subjects account. Money mules are often used in these schemes because they have access to financial institutions within the United States. In addition, they provide obfuscation for the actors because the funds received from victims are laundered through the money mules's accounts before being passed on to the actors.

11. Based on the aforementioned information, Affiant believes there is probable cause to believe that LEWIS has been serving as a "money mule" for "Jenny Glenn" in the course of a scheme to commit extortion against other persons. LEWIS and "Jenny Glenn" have discussed a number of exchanges of money transferred first to LEWIS and then to "Jenny Glenn." In particular, it appears from the evidence that Minor Victim was extorted by someone who obtained a nude image of Minor Victim and then forced Minor Victim to pay money in exchange for that nude image to not be released to others, which resulted in Minor Victim committing suicide. It also appears possible that LEWIS was involved in that scheme to extort Minor Victim based on evidence indicating money was transferred from Minor Victim directly to LEWIS through Venmo.

12. Based on the aforementioned information, Affiant believes there is probable cause to believe LEWIS has committed the offense of extortion, in violation of 18 U.S.C. § 875(d), and conspiracy to commit extortion, in violation of 18 U.S.C. § 371, and that there is probable cause

to believe that electronic devices that may be located at the SUBJECT PREMISES contain evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 371 and 875(d).

DEFINITIONS

13. I am aware that computer hardware and computer software may be utilized to store records which include, but are not limited to, those related to business activities, criminal activities, associate names and addresses, and the identity and location of assets illegally gained through criminal activity.

14. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

A. Written or printed matter of any kind, correspondence, memoranda, notes, diaries, statistics, letters, telephone toll records, telegrams, contracts, reports, checks, statements, receipts, returns, summaries, pamphlets, books, ledgers, journals, registers, records, vouchers, slips, bills, calendars, pads, notebooks, files, logs, lists, bulletins, credit materials, data bases, teletypes, telefaxes, invoices, worksheets; and

B. Graphic records or representations, photographs, slides, drawings, designs, graphs, charts, pictures, sketches, images, films, videotapes, and aural records or representations, tapes, records, disks.

15. The terms "records," "documents," and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications that may have been created or stored, including (but not limited to): any hand-made form (such as writing, drawing, painting, with any implement on any surface, directly or

indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); and any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, smart phones, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

USE OF COMPUTERS WITH CHILD EXPLOITATION

16. The development of computers and smart phones has added to the methods individuals use to interact with and sexually exploit children. Computers serve four functions in connection with child exploitation cases. These are: production of images, communication, distribution of images, and storage of images and communications.

17. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, smart phone, or mobile device, so that the image file is stored in his computer, phone, or mobile device.

18. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused

after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

19. The computer's capability to store images in digital form makes it an ideal repository for pornography. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera or camera on a phone to capture an image, process that image in a computer with a video capture board, and to save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

20. Smart phone technology, has expanded computer capability in recent years by allowing users to access the Internet via their phone. The smart phone user can search the Internet for specific files, check personal email accounts, log on to social networking sites, communicate with other computer users, compose and edit documents, produce photographic images, and store and view movie and picture files. Further, smart phone technology allows users to back the

contents of their phone up to a computer and transfer image files from their smart phone to a computer or other electronic device.

THE INTERNET AND TECHNICAL TERMS PERTAINING TO COMPUTERS

21. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet – for example, through a university, an employer, or a commercial service – which is called an "Internet Service Provider" or "ISP" (see definition of "Internet Service Provider" below). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit websites (see definition of "websites" below), and make purchases from them.

22. Set forth below are some definitions of technical terms, used throughout this Affidavit pertaining to the Internet and computers more generally:

A. Computer system and related peripherals, and computer media: As used in this affidavit, the terms "computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware,

computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, smart phones, mobile devices in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

B. Internet Service Providers (ISPs) and the Storage of ISP Records: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information,

account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," see 18 U.S.C. § 2510(17), and the provider of such a service is an "electronic communications service." An "electronic communications service," as defined by statute, is "any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." 18 U.S.C. § 2711(2).

C. Log File: Log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, log on/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was

accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEM

23. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting such as an office or laboratory. This is true because of the following:

A. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

B. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to

recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

24. Based upon my consultation with experts in computer searches, data retrieval from computers, and related media and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

A. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, data security devices are not necessary to retrieve

and preserve the data after inspection, the government will return them in a reasonable time.

B. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as central processing unit (CPU). In cases like this one where the evidence consists partly of graphics files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

C. In addition, there is probable cause to believe that the computer(s) and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime of extortion in violation of law, and should all be seized as such.

METHOD OF SEARCHING AND EXAMINING COMPUTERS AND DIGITAL EVIDENCE

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

A. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities

include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

B. *IP Address*: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in *the* range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

C. *Internet*: The Internet is a global network of computers and other electronic devices that *communicate* with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

26. Based on my training, experience, and research, I know that computers and smart phones have capabilities that allow it to serve as a device to facilitate communications via the Internet, and also retain files containing contraband, and other related documents and communications, including email communications. In my training and experience, examining data

stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. There is probable cause to believe that things that were once stored on the computer(s) and smart phone(s) may still be stored there, for at least the following reasons:

A. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been *downloaded* onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

C. Wholly apart from user-generated files, computer storage media-in particular, computers' internal hard drives-contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

D. *Forensic evidence*. As further described in the respective Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the computer(s) and smart phone(s) were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the items because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

E. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

F. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that

might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Additionally, if necessary, the warrant permits any electronic devices to be moved across state lines if necessary to conduct a forensic download the devices.

TECHNICAL INFORMATION REGARDING FACEBOOK

30. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. When signing up for a Facebook account, the user must agree to Facebook's terms of service titled "Statement of Rights and Responsibilities." Facebook's terms of service states, "You will not use Facebook to do anything unlawful, misleading, malicious or discriminatory."

31. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. The information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code) telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

32. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

33. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events and birthdays.

34. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments and links that will typically be visible to anyone who can view the user's profile.

35. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by the user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

36. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

37. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

38. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

39. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

40. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about the user's access or use of that application may appear on the user's profile page.

41. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends'

Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

42. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact the user viewed the profile and would show when and from what IP address the user did so.

43. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

44. The computers or servers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account activation.

45. Generally, when served with a search warrant for electronic communications, the electronic communications service provider (ECSP), such as Facebook, will send the contents of the specified account(s) to the investigating agency, usually on a CD or DVD, for the investigator to review. The ECSP can copy the contents of the entire account because that is within their expertise. Though the ECSP affirms that the records relate to the specified email account, the provider does not and will not undertake the examination of the contents of an email account to make a determination as to what is relevant or irrelevant to the investigation. Generally, and in this case particularly, the provider is not familiar with the investigation and is not in a position to identify the victim(s) or subject(s) of the investigation.

46. The provider is neither qualified nor trained to search the account information as would a law enforcement officer. Only a trained agent, familiar with the statutory violations and facts of the case, can determine what items should or should not be seized. For these reasons, your Affiant requests the provider disclose the records listed in Section 4, for the account(s) listed.

47. From Affiant's training and experience, Affiant knows that individuals with a sexual interest in children tend to engage multiple children at a time, trying to find a receptive minor. Because the nature of this criminal investigation involves the online enticement of a child, Affiant believes the account is likely to contain evidence of similar conduct with other minors, which may be found in a variety of locations, including but not limited to: friends lists, groups, status updates, wall posts, comments, events, birthdays, photos/videos, tags, private messages, notes/blogs, hyperlinks, gifts, pokes, classified ads, pending friend requests, and rejected friend requests. For this reason, the law enforcement investigator must be allowed to review all of the contents of the account for evidence of the crimes detailed below.

CONCLUSION

Based upon the foregoing, your Affiant respectfully submits that there is probable cause to believe that an individual, believed to be ISAIAH LEWIS, who resides at the SUBJECT PREMISES described above, has violated 18 U.S.C. § 875(d), that is extortion, and 18 U.S.C. § 371, that is conspiracy to commit extortion. Additionally, there is probable cause to believe that evidence of the commission of this offense is located in the SUBJECT PREMISES, and on the person of LEWIS if he is located in the SUBJECT PREMISES, described in Attachment A, and this evidence, listed in Attachment B, both incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offense.

FURTHER AFFIANT SAYETH NOT.

Ashley Davis, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me by telephone on this 14th day of October 2022.

HONORABLE JILL A. MORRIS
United States Magistrate Judge
Western District of Missouri